## REMARKS

Claims 17-66 and 73-122 are pending in the present application. Claims 113-122 have bean added as a result of this response. Claims 17, 22, 27, 32, 37, 42, 47, 52, 57, 62, and 113-122 are independent claims.

## 35 U.S.C. § 103(A) LIDL/QUISQUATER/RIVEST ET AL. REJECTION

Claim 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Dicpherment Algorithm for RSA Public-Key Cryptosystem, 1982); and Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest. This rejection, insofar as it pertains, to the presently pending claims, is respectfully traversed for the following reasons.

In formulating the rejection of claim 17 in view of Lidl, Quisquater, and Rivest, the Examiner picks and chooses various portions of three publications to piece together the subject matter of the present claims. In Applicants previous response, Applicants argued that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose the various teachings of Lidl, Quisquater, and Rivest, in order to piece together the invention recited in the presently pending claim.

In the present Office Action, the Examiner asserts on page 4, that one of ordinary skill in the art would be motivated to apply the Quisquater teachings to Lidl to improve the speed and use of computational resources.

Applicants respectfully submit that motivation may be found in one of three places:

1. the prior art references themselves;

2. the nature of the problem being solved; or

3. the knowledge of one of ordinary skill in the art.

Applicants respectfully assert that Lidl teaches absolutely nothing with respect to a desire to improve speed or save computational resources. Applicants further respectfully submit that Lidl is not solving a speed or computation problem. Applicants further respectfully submit that the Examiner has not established that such motivation would be within the realm of one of ordinary skill in the art. Accordingly, Applicants respectfully submit that the Examiner has failed to establish proper motivation for combining Quisquater and Lidl.

In the place of true motivation, the Examiner has created a motivation, which is not supported by any of the references of record. A creation, after the fact, of motivation, is improper hindsight. Applicants respectfully assert that the Examiner's rejection is fatally deficient for at least this reason.

The Examiner further relies on the Rivest et al. for teaching randomness and distinctness. However, Applicants respectfully assert that Rivest teaches nothing with regard to distinctness. The Examiner recognizes this in the paragraph bridging pages 4 and 5 of the Office Action and attempts to create a circular argument as to how Rivest teaches distinctness. However, Applicants respectfully assert that the fact remains that Rivest never mentions or infers that the two prime factors p and q need to be distinct and the Examiner's circular logic fails to infer such a teaching. Accordingly, Applicants respectfully submit that the Examiner's combination of references is deficient for at least this reason.

Still further, the Examiner asserts that one of ordinary skill in the art would combine Rivest and Lidl to maximize security. However, Lidl neither mentions maximum security nor indicates that maximum security recognizes maximum security as a problem. Accordingly, Applicants respectfully submit, for the reasons set forth above with respect to Quisquater and Lidl, the Examiner has also failed to establish proper motivation as to why one of ordinary skill in art would combine Rivest with Lidl. Accordingly, Applicants respectfully submit that claim 17 is allowable for at least this reason.

In defense of the Examiner's picking and choosing of references, on page 18 of the outstanding office action, the Examiner asserts that "...Rivest first suggested the method of using multiple primes and the CRT and Lidl set the steps out for the student and finally Quisquater and Courier show how to apply it for a faster algorithm. Thus rather than picking and choosing various portions of the prior art at random, Examiner merely is following a direction originally motivated and set forth by Rivest (in Lidl)."

For the reasons set forth above, the Examiner has not established motivation to combine, as Rivest is interested in maximum security, Quisquater in speed, and Lidl is nothing more than a basic text book, the alleged "direction" being fabricated by the Examiner. Accordingly, Applicants respectfully submit that the Examiner's combination of references is deficient for at least this reason.

## 35 U.S.C. § 103(A) LIDL/QUISQUATER/RIVEST ET AL./DING ET AL. REJECTION

Claims 18-66 and 73-92 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public -Key Cryptosystem, 1982); and Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et al. The Chinese Remainder Theorem, World Scientific. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

In formulating this rejection in view of Lidl, Quisquater, Rivest, and Ding, the Examiner again picks and chooses various portions of four publications to piece together the subject matter of the present claims. In Applicants previous response, Applicants argued that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Lidl, Quisquater, Rivest, and Ding, in order to piece together the invention recited in the presently pending claim.

With respect to Ding et al., Applicants still cannot find any reason on the record why one of ordinary skill in the art would combine Ding with any of Lidl, Quisquater, or Rivest and the Examiner has still failed to present such a reason. Although Ding is generally related to the Chinese Remainder Theorem and its applications in computing, coding and cryptography, the Examiner has failed to establish any concrete reasons why one of ordinary skill in the art would combine Ding with any of Lidl, Quisquater, or Rivest. Accordingly, Applicants respectfully submit that the Examiner's rejection is fatally deficient for at least this reason.

## 35 U.S.C. § 103(A) RSA/RIVEST ET AL./QUISQUATER/KNUTH REJECTION

Claim 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rivest et al. (US 4,405,829 A) henceforth RSA, and further in view of Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest; Quisquater, Fast Decipherment Algorithm for RSA Public-key Cryptosystem and further in view of Knuth, The Art of Computer Programming, Vol. 2, page 179. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

In formulating the rejection of claim 17 in view of RSA, Rivest, Quisquater, and Knuth, the Examiner picks and chooses various portions of four publications to piece together the subject matter of the present claims. In Applicants previous response, Applicants argued that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of RSA, Quisquater, Rivest, and Knuth in order to piece together the invention recited in the presently pending claim.

In paragraph 23, which is the only motivation advanced by the Examiner with respect to this rejection, the Examiner offers reasons why one of ordinary skill in the art would have been motivated to combine Lidl with Quisquater. However, Applicants respectfully submit that Lidl is not a reference used in this rejection. Accordingly, a discussion of it is misplaced. Applicants respectfully submit that the Examiner has failed to even advance a reason why one of ordinary skill in the art would combine RSA, Rivest, Quisquater, and/or Knuth. Accordingly, Applicants respectfully submit that the Examiner's rejection is fatally deficient for this reason.

## 35 U.S.C. § 103(A) RSA/QUISQUATER/RIVEST ET AL./DING ET AL. REJECTION

Claims 18-66 and 73-92 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rivest et al. (US 4,405,829 A) henceforth RSA, and further in view of Quisquater, Fast Decipherment Algorithm for RSA Public-Key Cryptosystem, 1982; and Rivest et al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et al. The Chinese Remainder Theorem, World Scientific. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed.

In formulating the rejection of claim 18-66 and 73-92 in view of RSA, Quisquater, Rivest, and Ding, the Examiner picks and chooses various portions of four publications to piece together the subject matter of the present claims. In Applicants previous response, Applicants argued that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of RSA, Quisquater, Rivest, and Ding, in order to piece together the invention recited in the presently pending claim.

With respect to claims 18-21 and 73-74, Applicants respectfully submit that this rejection is fatally deficient. In particular, in rejecting claim 17, upon which claims 18-21 and 73-74 depend, the Examiner uses RSA, Rivest, Quisquater and Knuth. In the rejection of claims 18-21 and 73-74, the Examiner uses RSA, Quisquater, Rivest et al., and Ding. However, if Knuth is necessary to reject independent claim 17, Knuth also must be necessary to reject claims which depend upon claims 17, namely, claims 18-21 and 73-74. Applicants respectfully submit that the Examiner's rejection is fatally deficient for at least this reason with respect to claims 18-21 and 73-74.

With respect to claims 22-66 and 75-92, the Examiner has again failed to advance any type of motivation as to why one of ordinary skill in the art would combine, RSA, Quisquater, Rivest and/or Ding. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

## 35 U.S.C. § 1203(A) NEMO/RIVEST ET AL./QUISQUATER REJECTION

Claims 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996; Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest; and Quisquater, Fast Decipherment Algorithm for RSA Public-key Cryptosystem, 1982. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

In the previous response, Applicants challenged the validity of Nemo as a reference. The copyright notice on Nemo states "The original version of this article may be obtained from Scientific Bulgarian magazine, August 1996." Applicants have performed extensive research with the Library of Congress, the British Library, and on the Internet and Applicants have been unable to identify "Scientific Bulgarian" as an actual publication.

It is settled law that a magazine is effective as a printed publication under 35 U.S.C. S § 102(b) as of the date it reached the addressee and not the date it was placed in the mail. MPEP § 70602. *Protein Foundation Inc. v. Brenner 151 USPQ 561(D.D.C. 1966).* Accordingly, Applicants respectfully assert that the "original version" of the NEMO article is not prior art since the Examiner has failed to establish Scientific Bulgarian as an actual magazine obtained by any addressee.

The NEMO article provided by the Examiner also includes a copyright "1996" date. An article with a year-only date should only be entitled to the last date of that year, namely December 31, 1996 unless the Examiner can establish otherwise. Applicants filing date is December 9, 1996. As a result, the Nemo publication is neither a 102(a) nor a 102(b) publication against the present application.

On page 17 of the Office Action, the Examiner asserts that "Scientific Bulgarian" is well know in the art as an indication of a paper being published under "copy left for scientific papers" and that the Nemo paper complies with those directives. Irrespective of these facts, the Examiner has not established that the Nemo publication has been "published" in such a manner that anyone who chose might avail themselves of the information it contains.

As set forth above, since Scientific Bulgarian was never mailed to any addressee, the original version of the Nemo article is not entitled to its August 1996 date. Further, since the date printed on the copy of the publication the Examiner supplied is 1996, the best date that can be attributed to this publication is December 31, 1996, which does not qualify prior art against the present application. Accordingly, Applicants respectfully submit that any rejection involving Nemo must be withdrawn.

Applicants further respectfully submit that if the Examiner intends to rely on Nemo as an "electronic publication", Applicant requests the Examiner to comply with the status as a printed publication and date of availability requirements of MPEP § 2128, namely the Examiner must:

1. produce sufficient proof of Nemo's dissemination or that Nemo has otherwise been available and accessible to persons concerned with the art to which the document relates and thus most likely to avail themselves of its contents; and

2. establish a date of Nemo's availability to such persons.

## 35 U.S.C. § 1203(A) NEMO/QUISQUATER/RIVEST ET AL./ DING ET AL. REJECTION

Claims 18-66 and 73-92 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996, and further in view of Quisquater, Fast Decipherment Algorithm for RSA Public -Key Cryptosystem, 1982); Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et al. The Chinese Remainder Theorem, World Scientific. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

Applicants respectfully submit that this rejection be withdrawn for at least the reasons set forth above with respect to Nemo above.

Applicants respectfully submit that the new claims 113-122 recite additional patentable features of the present invention. Allowance of claims 113-122 is respectfully requested.

## CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance of each of claims 17-66 and 73-122 in connection with the present application is earnestly solicited.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact John A. Castellano at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By ______________________________
John A. Castellano, Reg. No. 35,094
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/cah